Cassandra Crossing/ L'insostenibile inaffidabilità del Cloud

(315)— Sempre più aziende, istituzioni e pubbliche amministrazioni si rivolgono a soluzioni che operano sulla nuvola. Ma se i dati sono…

Cassandra Crossing/ L'insostenibile inaffidabilità del Cloud

(315)— Sempre più aziende, istituzioni e pubbliche amministrazioni si rivolgono a soluzioni che operano sulla nuvola. Ma se i dati sono esposti al tecnocontrollo, chi è disposto a fidarsi?

4 aprile 2014—Delle vittime e dei beneficiari dello scandalo Datagate si è parlato più che a sufficienza nei media: la notizia è ormai troppo sfruttata, anche se tanto rimarrebbe ancora da scrivere e da capire.

Nessuno però avrebbe messo in conto contraccolpi pesanti per un intero settore commerciale in tumultuosa crescita: i fornitori di servizi Cloud e SaaS, cioè coloro che mettono a disposizione risorse informatiche virtualizzate e raggiungibili in rete geografica (server, cpu, spazio disco etc.) o addirittura interi servizi software, da un database ad un'intera applicazione CRM.

Per le aziende significa esternalizzare la maggior parte dei servizi IT in un colpo solo, e spesso su un unico fornitore, con un occhio alle economie di bilancio e l'altro a sempre graditi tagli di teste nei servizi IT interni.

Persino le Pubbliche Amministrazioni ed i loro fornitori stavano iniziando ad orientarsi verso il Cloud, che prometteva non solo risparmi nei costi e guadagni in flessibilità, ma anche uno spruzzo di modernità di cui i loro servizi IT hanno sempre avuto molto bisogno.

L'onda lunga del Datagate, come un imprevisto tsunami, ha colpito anche loro.

Quale azienda con una vera proprietà intellettuale, fatta anche di segreti industriali e ricerca & sviluppo, affiderà mai i suoi dati ed il suo futuro ad aziende IT che sono state legalmente e segretamente coartate a fornire a terzi tutte le informazioni dei loro clienti? E se queste informazioni fossero state gli archivi di un nuovo prodotto o le mail di importantissime trattative industriali o legali in corso?

Non sarebbe la prima volta (Echelon docet) che dati intercettati per finalità di sicurezza nazionale si trasformano come per magia in vantaggio competitivo per le aziende della nazione intercettante.

Quale PA può prestare credito a garanzie legali sul trattamento dei dati posti nel Cloud, visto che le controparti sono obbligate a violarli ed a mantenere il segreto?

Certo, formalmente le Pubbliche Amministrazioni possono anche considerarle comunque valide, ma potrebbero in futuro essere loro contestate violazioni sostanziali, perché note e palesi, dei loro doveri di privacy e riservatezza.

Dulcis in fundo, i dati delle Pubbliche Amministrazioni e quelli più riservati ancora dello Stato sfumano gli uni negli altri: posto che la sicurezza nazionale si possa gestire con scelte commerciali, il Cloud sembra davvero l'ultima scelta da prendere in considerazione.

Un discreto marasma si è perciò creato nelle offerte dei fornitori di servizi Cloud: c'è stato chi ha delocalizzato server fisici in Europa per garantire un safe harbour nei confronti degli Stati Uniti, chi ha offerto soluzioni crittografiche più robuste come architettura (tipicamente

end-to-end), chi infine si è limitato ad inserire nuove clausole di non responsabilità nei contratti in essere, ed a farle accettare dai loro clienti.

Solo il tempo ci dirà se questa ondata si rivelerà una tempesta in un bicchier d'acqua e tutto tornerà come prima, o se la sicurezza e la privacy tecnologica, contrattuale e legale dei servizi Cloud cambieranno, magari migliorando.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on October 14, 2017.

Canonical link

Exported from Medium on August 27, 2025.